IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Currently Amended) A method for analyzing a network protocol stream for a security-related event, comprising:

identifying at least two valid states associated with ~~the~~ a network protocol in which a first host system communicating with a second host system using the network protocol may be placed;

defining at least one valid transition between a first state of the at least two valid states and a second state of the at least two valid states;

expressing the at least one valid transition in the form of a first regular expression;

defining an invalid state associated with the network protocol;

expressing as a second regular expression an invalid transition from the first state to the invalid state;

determining that a connection under the network protocol is in the first state; and

~~using the regular expression to analyze the network protocol stream by applying, based at least in part on the determination that the connection under the network protocol is in the first state, the regular expression~~ applying to a received packet associated with the connection:

the first regular expression to determine whether the packet is associated with the at least one valid transition, and

the second regular expression to determine whether the packet is associated with the invalid transition.

2.   (Currently Amended) A method for analyzing a network protocol stream as recited in claim 1, further comprising compiling the first regular expression into computer code.

3.   (Original)   A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises code in the C programming language.

4.   (Original)   A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises optimal computer code.

5.   (Original)   A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises nearly optimal computer code.

6.   (Currently Amended) A method for analyzing a network protocol stream as recited in claim 1, wherein using the first regular expression to analyze the network protocol stream comprises copying the network protocol stream to a third system and using the first regular expression to analyze the network protocol steam at the third system.

7.   (Original)   A method for analyzing a network protocol stream as recited in claim 6, wherein the network protocol stream comprises packets of data, each packet being associated with a sequence number indicating its position relative to other packets in the protocol stream, and the third system reassembles the packets into the order indicated by the respective sequence numbers of the packets received.

8.   (Original)   A method for analyzing a network protocol stream as recited in claim 7, wherein a copy of the network protocol stream is maintained in the third system until analysis has been completed.

9.   (Original)   A method for analyzing a network protocol stream as recited in claim 7, wherein in the event the packets are received by the third system in sequence number order, a copy is maintained in the third system only of those packets comprising the portion of the network protocol currently under analysis.

10.   (Currently Amended) A method for analyzing a network protocol stream as recited in claim 1, further comprising keeping track of which of the at least two valid states the first host system currently is in.

11.   (Currently Amended) A method for analyzing a network protocol stream as recited in claim 10, further comprising changing the tracked state of the first host system from the first of

the at least two <u>valid</u> states to the second of the at least two <u>valid</u> states in the event the analysis of the network protocol stream indicates the at least one valid transition has taken place.

12. (Cancelled)

13. (Currently Amended) A method for analyzing a network protocol stream as recited in claim ~~12~~ 1, wherein the invalid ~~operation may indicate~~ transition indicates that a security-related event has taken or is taking place.

14. (Cancelled)

15. (Currently Amended) A method for analyzing a network protocol stream as recited in claim ~~14~~ 1, further comprising:

keeping track of which state, from the set comprising the at least two <u>valid</u> states and the ~~further~~ invalid state, the first host system currently is in; and

changing the state of the first host system to the ~~further~~ invalid state in the event that the analysis of the network protocol stream indicates the invalid ~~operation~~ transition has taken place.

16. (Currently Amended) A method for analyzing a network protocol stream as recited in claim 15, further comprising providing, in the event that the analysis of the network protocol stream indicates the invalid ~~operation~~ transition has taken place, an indication that the invalid ~~operation~~ transition has taken place.

17. (Currently Amended) A method for analyzing a network protocol stream as recited in claim 15, further comprising discontinuing analysis of the network protocol stream once the state of the first host system has been changed to the ~~further~~ invalid state.

18. (Cancelled)

19. (Currently Amended) A system for analyzing a network protocol stream between a first host system and a second host system for a security-related event, the first host system being susceptible to being placed under the network protocol in one of at least two <u>valid</u> states associated with the network protocol, the system comprising:

a computer configured to:

receive a network protocol stream;

determine that a connection under the network protocol is in a first state of the at least two valid states; and

~~analyze the network protocol stream by~~ applying ~~, based at least in part on the determination that the connection under the network protocol is in the first state,~~ to a received packet associated with the connection ~~a regular expression, the~~:

a first regular expression corresponding to a valid transition from the first state of the at least two valid states to a second state of the at least two states, and

a second regular expression corresponding to an invalid transition from the first state of the at least two valid states to a predefined, invalid state; and

memory associated with the computer and configured to store the first regular expression.

20.   (Currently Amended) A system for analyzing a network protocol stream between a first host system and a second host system for a security-related event, the first host system being susceptible to being placed under the network protocol in one of at least two valid states associated with the network protocol, the system comprising:

means for receiving the network protocol stream; and

means for analyzing the network protocol stream by:

determining that a connection under the network protocol is in a first state of the at least two valid states; ~~and~~

applying ~~, based at least in part on the determination that the connection under the network protocol is in the first state,~~ to a received packet associated with the connection:

~~a regular expression, the~~ a first regular expression corresponding to a valid transition from the first state of the at least two valid states to a second state of the at least two valid states; and

a second regular expression, the second regular expression corresponding to an invalid transition from the first state of the at least two valid states to a pre-defined, invalid state .

21.   (Currently Amended) A computer program product for analyzing a network protocol stream, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

identifying at least two <u>valid</u> states in which a first host system communicating with a second host system using ~~the~~ <u>a</u> network protocol may be placed;

defining at least one valid transition between a first state of the at least two states and a second state of the at least two <u>valid</u> states;

expressing the at least one valid transition in the form of a <u>first</u> regular expression;

<u>defining an invalid state associated with the network protocol;</u>

<u>expressing as a second regular expression an invalid transition from the first state to the invalid state;</u>

determining that a connection under the network protocol is in the first state; and

~~using the regular expression to analyze the network protocol stream by applying, based at least in part on the determination that the connection under the network protocol is in the first state, the regular expression~~ <u>applying</u> to a received packet associated with the connection<u>:</u>

<u>the first regular expression</u> to determine whether the packet is associated with the at least one valid transition<u>, and</u>

<u>the second regular expression to determine whether the packet is associated with the invalid transition.</u>

22.   (Cancelled)

INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on 09/30/05 between the Examiner and the Applicants' undersigned representative. The Office Action mailed on 07/01/05 was discussed. Specifically, the rejections of claims 1 and 18 in light of I'Anson and the proposed amendments set forth herein were discussed with the intent to place the claims in better condition for allowance or appeal.

The Applicants wish to thank the Examiner for his time and attention in this case.